communication, and other factors that may affect the accuracy or integrity of information furnished to consumer reporting agencies.

(m) Complying with applicable requirements under the Fair Credit Reporting Act and its implementing regulations.

[74 FR 31524, July 1, 2009]

APPENDICES F–I TO PART 717 [RESERVED]

APPENDIX J TO PART 717—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

Section 717.90 of this part requires each federal credit union that offers or maintains one or more covered accounts, as defined in §717.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist federal credit unions in the formulation and maintenance of a Program that satisfies the requirements of §717.90 of this part.

I. The Program

In designing its Program, a federal credit union may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to members or to the safety and soundness of the federal credit union from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A federal credit union should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Federal credit unions should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the federal credit union has experienced;

(2) Methods of identity theft that the federal credit union has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from members, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the federal credit union.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating members, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the federal credit union has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a federal credit union should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a member's account records held by the federal credit union or a third party, or notice that a member has provided information related to a covered account held by the federal credit union to someone fraudulently claiming to represent the federal credit union or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the member;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;